EXHIBIT A

2023 IL 128004

Supreme Court of Illinois.

LATRINA COTHRON, Appellee,

v.

WHITE CASTLE SYSTEM, INC., Appellant.

(Docket No. 128004)

|

Opinion filed February 17, 2023.

OPINION

JUSTICE ROCHFORD delivered the judgment of the court, with opinion.

***1** ¶ 1 This case requires us to construe section 15(b) and 15(d) of the Biometric Information Privacy Act (Act) (740 ILCS 14/15(b), (d) (West 2018)) in an action alleging that an employer violated the Act when it repeatedly collected fingerprints from an employee and disclosed that biometric information to a third party without consent. Specifically, the United States Court of Appeals for the Seventh Circuit certified the following question of law to this court: "Do section 15(b) and 15(d) claims accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only upon the first scan and first transmission?" *Cothron v. White Castle System, Inc.*, 20 F.4th 1156, 1167 (7th Cir. 2021). We hold that a separate claim accrues under the Act each time a private entity scans or transmits an individual's biometric identifier or information in violation of section 15(b) or 15(d).

¶ 2 I. BACKGROUND

¶ 3 We recite the facts as provided by the Seventh Circuit in its certification ruling. See, *e.g.*, *In re Hernandez*, 2020 IL 124661, ¶ 5. The controversy arises from a proposed class action filed by plaintiff, Latrina Cothron, on behalf of all Illinois employees of defendant, White Castle System, Inc. (White Castle). Plaintiff originally filed her action in the circuit court of Cook County against White Castle and its third-party vendor, Cross Match Technologies. Cross Match Technologies removed the case to federal court under the Class Action Fairness Act of 2005 (28 U.S.C. §§ 1332(d), 1453 (2018)). Plaintiff later voluntarily dismissed Cross Match Technologies from her action and proceeded solely against White Castle in the United States District Court for the Northern District of Illinois.

¶ 4 According to her complaint, plaintiff is a manager of a White Castle restaurant in Illinois, where she has been employed since 2004. Shortly after her employment began, White Castle introduced a system that required its employees to scan their fingerprints to access their pay stubs and computers. A third-party vendor then verified each scan and authorized the employee's access.

¶ 5 Generally, plaintiff's complaint alleged that White Castle implemented this biometric-collection system without obtaining her consent in violation of the Act (740 ILCS 14/1 *et seq.* (West 2018)), which became effective in 2008 (see Pub. Act 95-994, § 1 (eff. Oct. 3, 2008)). Section 15(b) of the Act provides that a private entity may not "collect, capture, purchase, receive through trade, or otherwise obtain" a person's biometric data without first providing notice to and receiving consent from the person. 740 ILCS 14/15(b) (West 2018). Section 15(d) provides that a private entity may not "disclose, redisclose, or otherwise disseminate" biometric data without consent. *Id.* § 15(d).

¶ 6 Plaintiff asserted that White Castle did not seek her consent to acquire her fingerprint biometric data until 2018, more than a decade after the Act took effect. Accordingly, plaintiff claimed that White Castle unlawfully collected her biometric data and unlawfully disclosed her data to its third-party vendor in violation of section 15(b) and 15(d), respectively, for several years.

***2** ¶ 7 In relevant part, White Castle moved for judgment on the pleadings, arguing that plaintiff's

action was untimely because her claim accrued in 2008, when White Castle first obtained her biometric data after the Act's effective date. Plaintiff responded that a new claim accrued each time she scanned her fingerprints and White Castle sent her biometric data to its third-party authenticator, rendering her action timely with respect to the unlawful scans and transmissions that occurred within the applicable limitations period.

¶ 8 The district court agreed with plaintiff and denied White Castle's motion. *Cothron v. White Castle System, Inc.*, 477 F. Supp. 3d 723, 734 (N.D. Ill. 2020). The court later certified its order for immediate interlocutory appeal, finding that its decision involved a controlling question of law on which there is substantial ground for disagreement.

¶ 9 The United States Court of Appeals for the Seventh Circuit accepted the certification. After determining that plaintiff had standing to bring her action in federal court under article III of the United States Constitution (U.S. Const., art. III), the Seventh Circuit addressed the parties' respective arguments on the accrual of a claim under the Act. *Cothron*, 20 F.4th at 1162-65. Ultimately, the Seventh Circuit found the parties' competing interpretations of claim accrual reasonable under Illinois law, and it agreed with plaintiff that "the novelty and uncertainty of the claim-accrual question" warranted certification of the question to this court. *Id.* at 1165-66. The Seventh Circuit observed that the answer to the claim-accrual question would determine the outcome of the parties' dispute, this court could potentially side with either party on the question, the question was likely to recur, and it involved a unique Illinois statute regularly applied by federal courts. *Id.* at 1166. Thus, finding the relevant criteria favored certification of the question, the Seventh Circuit certified the question to this court.[1] *Id.* at 1166-67.

[1] Several federal district courts have stayed proceedings pending a final decision from the Seventh Circuit in *Cothron* in connection with the accrual question. See, *e.g.*, *Callendar v. Quality Packaging Specialists International, Inc.*, No. 21-cv-505-SMY, 2021 WL 4169967 (S.D. Ill. Aug. 27, 2021); *Hall v. Meridian Senior Living, LLC*, No. 21-cv-55-SMY, 2021 WL 2661521 (S.D. Ill. June 29, 2021); *Roberson v. Maestro Consulting Services, LLC*, No. 20-CV-00895-NJR, 2021 WL 1017127 (S.D. Ill, Mar. 17, 2021); *Roberts v. Graphic Packaging International, LLC*, No. 21-CV-750-DWD, 2021 WL 3634172 (S.D. Ill. Aug. 17, 2021); *Starts v. Little Caesar Enterprises, Inc.*, No. 19-cv-1575, 2021 WL 4988317 (N.D. Ill. Oct. 19, 2021); *Treadwell v. Power Solutions International, Inc.*, No. 18-cv-8212, 2021 WL 5712186 (N.D. Ill. Dec. 2, 2021).

¶ 10 We chose to answer that question. See Ill. S. Ct. R. 20(a) (eff. Aug. 1, 1992). The Illinois Chamber of Commerce, Chamber of Commerce of the United States, Retail Litigation Center, Inc., Restaurant Law Center, National Retail Federation, Illinois Manufacturers' Association, National Association of Manufacturers, Illinois Health and Hospital Association, Illinois Retail Merchants Association, Chemical Industry Council of Illinois, Illinois Trucking Association, Mid-West Truckers Association, and Chicagoland Chamber of Commerce were granted leave to file *amicus curiae* briefs in support of White Castle's position. Ill. S. Ct. R. 345 (eff. Sept. 20, 2010). The American Association for Justice, Employment Law Clinic of the University of Chicago Law School's Edwin F. Mandell Legal Aid Clinic, NELA/Illinois National Employment Law Project, Raise the Floor Alliance, and Electronic Privacy Information Center (EPIC) were granted leave to file *amicus curiae* briefs in support of plaintiff's position. *Id.*

¶ 11 II. ANALYSIS

***3** ¶ 12 The certified question asks: "Do section 15(b) and 15(d) claims accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only upon the first scan and first transmission?" When answering this question, we assume, without deciding, that White Castle's alleged collection of plaintiff's fingerprints and transmission to a third party was done in violation of the Act.

¶ 13 Section 15(b) of the Act provides:

> "No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative." 740 ILCS 14/15(b) (West 2018).

¶ 14 Section 15(d) of the Act provides, in relevant part, that

> "[n]o private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:
>
> *** the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure[.]" *Id.* § 15(d)(1).

¶ 15 Relevant to this case, the Act further defines the term "biometric identifier" to include a fingerprint and the term "biometric information" to include any information based on an individual's biometric identifier used to identify that person. *Id.* § 10. The Act provides a private right of action for any person aggrieved by a violation of the Act. *Id.* § 20.

¶ 16 White Castle argues that section 15(b) and 15(d) claims can accrue only once—when the biometric data is initially collected or disclosed. Section 15(b) provides that no private entity "may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, *unless it first*" provides notice and receives consent as outlined in the rest of section 15(b). (Emphasis added.) *Id.* § 15(b). According to White Castle, the "unless it first" phrase refers to a singular point in time; notice and consent must precede, or occur before, collection. The active verbs used in section 15(b)—collect, capture, purchase, receive, and obtain—all mean to gain control, an action that White Castle argues can only happen once under the plain meaning of those terms.

¶ 17 White Castle advances a similar argument for section 15(d), noting that it provides that no private entity "in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless" the private entity has obtained consent or certain exceptions apply. *Id.* § 15(d). Thus, section 15(d) requires consent in order for a private entity to "disclose, redisclose, or otherwise disseminate" an individual's biometrics. According to White Castle, the plain meaning of each verb used in section 15(d) "implicates the disclosure of biometrics by one party to a new, third party—said differently, a party that has not previously possessed the relevant biometric identifier or biometric information." As it argues for section 15(b) claims, White Castle contends that occurs only on the first instance of disclosure or dissemination.

***4** ¶ 18 Plaintiff responds that the plain meaning of the statutory language demonstrates that claims under section 15(b) and 15(d) accrue every time a private entity collects or disseminates biometrics without prior informed consent. According to plaintiff, this construction is consistent with the plain meaning of the statutory language, gives effect to every word in the provision, and directly reflects legislative intent to provide an individual with a meaningful and informed opportunity to decline the collection or dissemination of their biometrics. It also provides an incentive for private entities that collect biometric information to take action to mitigate their conduct if they neglected to comply at first.

¶ 19 Plaintiff maintains that section 15(b) applies to every instance when a private entity collects biometric information without prior consent. According to plaintiff, the word "first" in section 15(b) modifies the words "informs" and "receives." Thus, according

to plaintiff, an entity violates section 15(b) when it collects, captures, or otherwise obtains a person's biometrics without prior informed consent. Plaintiff observes that our appellate court reached the same conclusion in *Watson v. Legacy Healthcare Financial Services, LLC*, 2021 IL App (1st) 210279, ¶ 53. Similarly, section 15(d) prohibits the disclosure, redisclosure, or dissemination of biometrics by a private entity "unless" that entity receives prior consent. Thus plaintiff argues that, under the plain language of both section 15(b) and 15(d), a claim accrues each time that biometric identifiers or information are collected or disseminated by a private entity without prior informed consent.

¶ 20 To resolve the parties' dispute and answer the certified question, we focus on the language of the Act itself. The cardinal principle and primary objective in construing a statute is to ascertain and give effect to the intention of the legislature. *Roberts v. Alexandria Transportation, Inc.*, 2021 IL 126249, ¶ 29. The best indicator of legislative intent is the statutory language itself, given its plain and ordinary meaning. *In re Hernandez*, 2020 IL 124661, ¶ 18. Where the language is clear and unambiguous, we must apply the statute without resort to further aids of statutory construction. *Krohe v. City of Bloomington*, 204 Ill. 2d 392, 395 (2003). Only if the statutory language is ambiguous may we look to other sources to ascertain the legislature's intent. *Id.*

¶ 21 Section 15(b)

¶ 22 Section 15(b) mandates informed consent from an individual before a private entity collects biometric identifiers or information. Specifically, section 15(b) provides that "[n]o private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information unless it first" obtains informed consent from the individual or the individual's legally authorized representative. 740 ILCS 14/15(b) (West 2018).

¶ 23 We agree with plaintiff that the plain language of the statute supports her interpretation. "Collect" means to "to receive, gather, or exact from a number of persons or other sources." Webster's Third New International Dictionary 444 (1993). "Capture" means "to take, seize, or catch." *Id.* at 334. We disagree with defendant that these are things that can happen only once. As plaintiff explains in her complaint, White Castle obtains an employee's fingerprint and stores it in its database. The employee must then use his or her fingerprint to access paystubs or White Castle computers. With the subsequent scans, the fingerprint is compared to the stored copy of the fingerprint. Defendant fails to explain how such a system could work without collecting or capturing the fingerprint every time the employee needs to access his or her computer or pay stub. As the district court explained, "[e]ach time an employee scans her fingerprint to access the system, the system must capture her biometric information and compare that newly captured information to the original scan (stored in an off-site database by one of the third-parties with which White Castle contracted)." *Cothron*, 477 F. Supp. 3d at 732. To the extent White Castle is suggesting that "collection" or "capture" occurs only when an entity first obtains a print to store in its database—and subsequent authentication scans therefore cannot be collections or captures—this argument is belied by the position White Castle took below. White Castle acknowledges that it argued in its motion for judgment on the pleadings that plaintiff's claim accrued, if ever, in 2008 with her first scan after the Act's enactment. And White Castle argues in its brief that "there was no 'loss of control' under [the Act] until 2008, the first time she used the finger-scan technology in 2008 following [the Act's] effective date." Because White Castle first obtained a copy of plaintiff's fingerprint years before this, the first scan after the Act went into effect would have been a routine authentication scan. A claim could have accrued upon the taking of this authentication scan only if it were a collection or a capture under section 15(b). Moreover, section 15(b)(2) of the Act distinguishes between collection and storage. This section provides that the private entity must notify the subject of the "length of term for which a biometric identifier or biometric information is being collected, stored, and used." 740 ILCS 14/15(b)(2) (West 2008). That the subject must be notified how long his or her biometric data will be collected shows that the legislature contemplated collection as being something that would happen more than once.

***5** ¶ 24 We agree with the federal district court that "[a] party violates Section 15(b) when it collects, captures, or otherwise obtains a person's biometric information without prior informed consent. This is true the first time an entity scans a fingerprint or otherwise collects biometric information, but it is no less true with each subsequent scan or collection." *Cothron*, 477 F. Supp. 3d at 732. Our appellate court has reached the same conclusion, determining that "the plain language of [section 15(b)] establishes that it applies to each and every capture and use of plaintiff's fingerprint or hand scan. Almost every substantive section of the Act supports this finding." *Watson*, 2021 IL App (1st) 210279, ¶ 46.

¶ 25 White Castle's suggestion that the "unless it first" phrase in section 15(b) refers only to the first collection of biometric information is inaccurate. Contrary to White Castle's position, the "unless it first" phrase refers to the private entity's statutory obligation to obtain consent or a release. See 740 ILCS 14/15(b) (West 2018) (prohibiting a private entity from collecting, capturing, purchasing, receiving, or otherwise obtaining biometric information "unless it first" obtains consent or a release as described by the statute). As our appellate court correctly determined, the "unless it first" phrase "modifies the entity's obligations, not the triggering actions." *Watson*, 2021 IL App (1st) 210279, ¶ 53.

¶ 26 Section 15(d)

¶ 27 Similar to section 15(b), section 15(d) mandates consent or legal authorization before a specific action is taken. It provides that "[n]o private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless" it obtains informed consent from the individual or their legal representative or has other legal authorization to disclose that information. 740 ILCS 14/15(d) (West 2018).

¶ 28 As with section 15(b), we conclude that the plain language of section 15(d) applies to every transmission to a third party. White Castle argues that a disclosure is something that can happen only once. The Seventh Circuit asserted that the plain meaning of "disclose" connotes a new revelation. See *Cothron*, 20 F.4th at 1163; see also Webster's Third New International Dictionary 645 (1993) (defining "disclose" as "to make known" or "to reveal *** something that is secret or not generally known"). In determining that an entity violates section 15(d) every time it discloses or otherwise disseminates biometric data, the district court focused on this section's use of the term "redisclose." *Cothron*, 477 F. Supp. 3d at 733. The district court agreed with plaintiff that repeated transmissions to the same third party are "redisclosures." *Id.* As the Seventh Circuit court pointed out, however, the issue is not quite so simple:

> "[Cothron] reads the term 'redisclose' as used in section 15(d) to include repeated disclosures of the same biometric data to the same third party. For its part, White Castle offers a different interpretation of the term: a downstream disclosure carried out by a third party to whom information was originally disclosed. That reading is consistent with the term 'redisclose' as used in other Illinois statutes.[2] Countering again, Cothron argues that this usage would make 'redisclose' meaningless surplusage. Section 15(d) applies to any 'private entity in possession of a biometric identifier or biometric information.' As such, a violation by a down-stream entity can just be called a 'disclosure,' making 'redisclose' redundant under White Castle's reading. Maybe so; or maybe 'redisclose' serves to make certain that down-stream entities are subject to section 15(d). See *Reid Hosp. & Health Care Servs., Inc. v. Conifer Revenue Cycle Sols., LLC*, 8 F.4th 642, 652 (7th Cir. 2021) (noting the tension between the anti-surplusage canon and the belt-and-suspenders drafting approach)." *Cothron*, 20 F.4th at 1164.

[2] See, *e.g.*, section 35.3(b) of the Children and Family Services Act (20 ILCS 505/35.3(b) (West 2020) ("[a] person to whom disclosure of a foster parent's name, address, or telephone number is made under this Section shall not redisclose that information except as provided in this Act or the Juvenile Court Act of 1987")) and section 5 of the Mental Health and Developmental Disabilities Confidentiality Act (740 ILCS

> 110/5(d) (West 2020) ("[n]o person or agency to whom any information is disclosed under this Section may redisclose such information unless the person who consented to the disclosure specifically consents to such redisclosure")). In its reply brief, White Castle lists several other Illinois statutes that use the term "redisclose" in the same manner.

***6** ¶ 29 We note that, even in the dictionary relied upon by White Castle, the principal meaning of "redisclose" is "[t]o disclose again." See WordSense Dictionary, https://www.wordsense.eu/redisclose/ (last visited Jan. 7, 2023) [https://perma.cc/ 63VU-RRTK]. Nevertheless, we do not believe that we have to specifically determine the meaning of "redisclose" in section 15(d) because the other terms in that section are broad enough to include repeated transmissions to the same party. "Disclose" also means to "expose to view" (Webster's Third New International Dictionary 645 (1993)), and Webster's gives as an example something happening more than once: "the curtain rises to [disclose] *once again* the lobby" (emphasis added) (*id.*). A fingerprint scan system requires a person to expose his or her fingerprint to the system so that the print may be compared with the stored copy, and this happens each time a person uses the system. Moreover, section 15(d) has a catchall provision that broadly applies to any way that an entity may "otherwise disseminate" a person's biometric data. "Disseminate" means "to spread or send out freely or widely." *Id.* at 656. White Castle asserts that this is something that can happen only once but provides no definitional support for that assertion. Thus, we find that the plain language of section 15(d) supports the conclusion that a claim accrues upon each transmission of a person's biometric identifier or information without prior informed consent.

¶ 30 We agree with the district court's explanation of how sections 15(b) and (d) are violated:

> "Section 15(b) provides that no private entity 'may collect, capture, purchase, receive through trade, or otherwise obtain' a person's biometric information unless it first receives that person's informed consent. 740 ILCS 14/15(b). This requirement is violated—fully and immediately—when a party collects biometric information without the necessary disclosure and consent. Similarly, Section 15(d) states that entities in possession of biometric data may only disclose or 'otherwise disseminate' a person's data upon obtaining the person's consent or in limited other circumstances inapplicable here. 740 ILCS 14/15(d). Like Section 15(b), an entity violates this obligation the moment that, absent consent, it discloses or otherwise disseminates a person's biometric information to a third party." *Cothron*, 477 F. Supp. 3d at 730-31.

We believe that the plain language of section 15(b) and 15(d) demonstrates that such violations occur with every scan or transmission.

¶ 31 White Castle's Other Arguments

¶ 32 We are not persuaded by White Castle's nontextual arguments in support of its single-accrual interpretation. Citing *Feltmeier v. Feltmeier*, 207 Ill. 2d 263 (2003), White Castle maintains that under Illinois law a claim accrues when a legal right is invaded and an injury inflicted. White Castle maintains that this court's decisions interpreting the Act define a right to secrecy in and control over biometric data and define the "injury" as loss of control or secrecy.

¶ 33 Citing *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, ¶¶ 33-34, White Castle contends that the Act allows a claim for an individual's loss of the "right to control" biometric information and that, once an individual loses control over the secrecy in his or her biometric information, it cannot be recreated, resulting in the loss of any confidentiality. See also *West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan, Inc.*, 2021 IL 125978, ¶ 46 (explaining that the Act protects a "secrecy interest"); *McDonald v. Symphony Bronzeville Park, LLC*, 2022 IL 126511, ¶ 24 (reiterating that the Act protect an individual's " 'right to privacy in and control over their biometric identifiers and biometric information' " (quoting *Rosenbach*, 2019 IL 123186, ¶ 33)).

¶ 34 Relying on this precedent, White Castle contends that, when a party collects or discloses biometric information without complying with the Act's notice and consent requirements, an individual's rights have

been invaded, an injury has occurred, and the plaintiff may immediately sue. In other words, "the invasion and injury are one and the same and occurred upon [p]laintiff's initial loss of control of her biometrics." For purposes of claim accrual under sections 15(b) and 15(d), White Castle argues that the claim accrues only on the initial scan or transmission of biometric information. Because a person cannot keep information secret from another entity that already has it, White Castle contends that the loss of an individual's right to control his or her biometrics is a "single overt act" that encompasses both the invasion of the interest and the infliction of the injury. See *Feltmeier*, 207 Ill. 2d at 279. Thus, a claim under section 15(b) or 15(d) can accrue only the first time the information is collected or disclosed. We disagree.

***7** ¶ 35 White Castle misreads our decisions in *Rosenbach*, *West Bend Mutual Insurance Co.*, and *McDonald*. As a preliminary observation, we note that none of those decisions involved, let alone analyzed, the question of claim accrual under the Act.

¶ 36 In fact, we find that *Rosenbach* supports our construction of sections 15(b) and 15(d). This court recognized in *Rosenbach* that the Act operates to codify an individual's right to privacy in and control over his or her biometric identifiers and information. *Rosenbach*, 2019 IL 123186, ¶ 33. Importantly, we determined in *Rosenbach* that a person is "aggrieved" or injured under the Act "when a private entity fails to comply with one of section 15's requirements." *Id.*

¶ 37 Focusing on the section 15 violation in *Rosenbach*, the same provision at issue in this case, we determined that, "[w]hen a private entity fails to comply with one of section 15's requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach." *Id.* Critically, *Rosenbach* explains that an individual raising a section 15 claim is not required to plead or prove actual damages because the statutory violation, "in itself, is sufficient to support the individual's or customer's statutory cause of action." *Id.*

¶ 38 Thus, contrary to White Castle's position, *Rosenbach* does not stand for the proposition that the "injury" for a section 15 claim is predicated on, or otherwise limited to, an initial loss of control or privacy. Instead, *Rosenbach* clearly recognizes the statutory violation itself is the "injury" for purposes of a claim under the Act, which is entirely consistent with our decision here. Our subsequent decisions in *West Bend Mutual Insurance Co.* and *McDonald* adhered to *Rosenbach*'s construction of the Act and similarly recognized that a claim under the Act is a private cause of action based exclusively on a statutory violation. *West Bend Mutual Insurance Co.*, 2021 IL 125978, ¶ 46 (citing *Rosenbach*); *McDonald*, 2022 IL 126511, ¶ 23 (citing *Rosenbach*).

¶ 39 Put simply, our caselaw holds that, for purposes of an injury under section 15 of the Act, the court must determine whether a statutory provision was violated. Consequently, we reject White Castle's argument that we should limit a claim under section 15 to the first time that a private entity scans or transmits a party's biometric identifier or biometric information. No such limitation appears in the statute. We cannot rewrite a statute to create new elements or limitations not included by the legislature. *Zahn v. North American Power & Gas, LLC*, 2016 IL 120526, ¶ 15.

¶ 40 White Castle and *amici* supporting White Castle's position caution this court against construing section 15(b) and section 15(d) to mean that a claim accrues for each scan or transmission of biometric information made in violation of those provisions. They assert that, because section 20 of the Act sets forth liquidated damages that a party may recover for "each violation," allowing multiple or repeated accruals of claims by one individual could potentially result in punitive and "astronomical" damage awards that would constitute "annihilative liability" not contemplated by the legislature and possibly be unconstitutional. For example, White Castle estimates that if plaintiff is successful and allowed to bring her claims on behalf of as many as 9500 current and former White Castle employees, class-wide damages in her action may exceed $17 billion. We have found, however, that the statutory language clearly supports plaintiff's position. As the district court observed, this court has repeatedly held that, where statutory language is clear, it must be given effect, " 'even though the consequences may be harsh, unjust, absurd or unwise.' " (Emphasis omitted.)

Cothron, 477 F. Supp. 3d at 734 (quoting *Peterson v. Wallach*, 198 Ill. 2d 439, 447 (2002)).

***8** ¶ 41 This court has repeatedly recognized the potential for significant damages awards under the Act. *Rosenbach*, 2019 IL 123186, ¶¶ 36-37; *McDonald*, 2022 IL 126511, ¶ 48. This court explained that the legislature intended to subject private entities who fail to follow the statute's requirements to substantial potential liability. *Rosenbach*, 2019 IL 123186, ¶ 36. The purpose in doing so was to give private entities "the strongest possible incentive to conform to the law and prevent problems before they occur." *Id.* ¶ 37. As the Seventh Circuit noted, private entities would have "little incentive to course correct and comply if subsequent violations carry no legal consequences." *Cothron*, 20 F.4th at 1165.

¶ 42 All of that said, we generally agree with our appellate court's recognition that "[a] trial court presiding over a class action—a creature of equity—would certainly possess the discretion to fashion a damage award that (1) fairly compensated claiming class members and (2) included an amount designed to deter future violations, without destroying defendant's business." *Century Mutual Insurance Co. v. Tracy's Treasures, Inc.*, 2014 IL App (1st) 123339, ¶ 72. It also appears that the General Assembly chose to make damages discretionary rather than mandatory under the Act. See 740 ILCS 14/20 (West 2018) (detailing the amounts and types of damages that a "prevailing party *may* recover" (emphasis added)); see also *Watson*, 2021 IL App (1st) 210279, ¶ 66 n.4 (concluding that damages under the Act are discretionary rather than mandatory). While we explained in *Rosenbach* that "subjecting private entities who fail to follow the statute's requirements to substantial potential liability, including liquidated damages, injunctions, attorney fees, and litigation expenses 'for each violation' of the law" is one of the principal means that the Illinois legislature adopted to achieve the Act's objectives of protecting biometric information (*Rosenbach*, 2019 IL 123186, ¶ 36 (quoting 740 ILCS 14/20 (West 2016))), there is no language in the Act suggesting legislative intent to authorize a damages award that would result in the financial destruction of a business.

¶ 43 Ultimately, however, we continue to believe that policy-based concerns about potentially excessive damage awards under the Act are best addressed by the legislature. See *McDonald*, 2022 IL 126511, ¶¶ 48-49 (observing that violations of the Act have the potential for "substantial consequences" and large damage awards but concluding that "whether a different balance should be struck *** is a question more appropriately addressed to the legislature"). We respectfully suggest that the legislature review these policy concerns and make clear its intent regarding the assessment of damages under the Act.

¶ 44 III. CONCLUSION

¶ 45 In sum, we conclude that the plain language of section 15(b) and 15(d) shows that a claim accrues under the Act with every scan or transmission of biometric identifiers or biometric information without prior informed consent.

¶ 46 Certified question answered.

Justices Neville, Cunningham, and O'Brien concurred in the judgment and opinion.

Justice Overstreet dissented, with opinion, joined by Chief Justice Theis and Justice Holder White.

¶ 47 JUSTICE OVERSTREET, dissenting:

¶ 48 I respectfully disagree with my colleagues' answer to the certified question. The majority's interpretation cannot be reconciled with the plain language of the statute, the purposes behind the Biometric Information Privacy Act (Act) (740 ILCS 14/1 *et seq.* (West 2018)), or this court's case law, and it will lead to consequences that the legislature could not have intended. Moreover, the majority's interpretation renders compliance with the Act especially burdensome for employers. This court should answer the certified question by saying that a claim accrues under section 15(b) or 15(d) of the Act (*id.* § 15(b), (d)) only upon the first scan or transmission.

***9** ¶ 49 The principles guiding our analysis are set forth in *Feltmeier v. Feltmeier*, 207 Ill. 2d 263, 278-79 (2003). This court held that, generally, "a limitations period begins to run when facts exist that authorize

one party to maintain an action against another." *Id.* at 278. Moreover, "where there is a single overt act from which subsequent damages may flow, the statute begins to run on the date the defendant invaded the plaintiff's interest and inflicted injury." *Id.* at 279. Thus, to resolve the question of when claims accrue under section 15(b) and (d), we must consider whether plaintiff has alleged a single overt act from which subsequent damages may flow.

¶ 50 Two considerations inform this inquiry: (1) what interests does the Act seek to protect and (2) what constitutes a violation of section 15(b) or (d) under the plain language of those provisions? This court has addressed the first question several times. In *Rosenbach*, this court explained that "[t]he Act vests in individuals and customers the right to control their biometric information by requiring notice before collection and giving them the power to say no by withholding consent." *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, ¶ 34. This court further explained that the "precise harm" the legislature sought to prevent was an individual's loss of the right to maintain biometric privacy. *Id.* In *West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan, Inc.*, 2021 IL 125978, ¶ 46, this court stated that the Act "protects a secrecy interest," such as an individual's right to "keep his or her personal identifying information like fingerprints secret." Finally, in *McDonald v. Symphony Bronzeville Park, LLC*, 2022 IL 126511, ¶ 24 (quoting *Rosenbach*, 2019 IL 123186, ¶ 33), this court reiterated that the Act protects an individual's " 'right to privacy in and control over their biometric identifiers and biometric information.' "

¶ 51 Turning to the language of the statute, section 15(b) requires certain disclosures to be made, and a written release obtained, before that entity may "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(b) (West 2018). The statute thus broadly applies to any way that a private entity obtains a person's or customer's biometric information without consent. It is axiomatic, however, that a private entity may obtain any one type of a person's biometric information only once, at least until that biometric identifier or information is destroyed. With subsequent authentication scans, the private entity is not obtaining anything it does not already have. The majority commits the same analytical error as the appellate court in *Watson v. Legacy Healthcare Financial Services, LLC*, 2021 IL App (1st) 210279.

¶ 52 The *Watson* court held that section 15(b) means that "an entity must inform a subject and receive a release 'before' it collects or captures. *** [T]here is no temporal limitation on 'collects' or 'captures,' thereby applying to the first, as well as the last, collection or capture." *Id.* ¶ 57. *Watson*'s error is in assuming that the private entity is collecting or capturing a person's biometric information with every scan. The majority makes the same error, equating every scan with a "collection." *Supra* ¶ 24. But this is not correct. Again, section 15(b) broadly applies to any way that a private entity obtains a person's biometric identifier or information. But this can happen only once. Here, White Castle obtains an employee's biometric identifier the first time that a fingerprint is scanned. White Castle is obviously not obtaining it with subsequent scans—White Castle already has it. As plaintiff acknowledges in her complaint, White Castle obtains an employee's fingerprint and stores it in its database. The employee is then required to use his or her fingerprint to access paystubs or White Castle computers. With the subsequent scans, the fingerprint is not being obtained, it is being compared to the fingerprint that White Castle already has. This fact is made plain in plaintiff's complaint. Plaintiff states, "Plaintiff was required to scan and register her fingerprint(s) so *White Castle could use them as an authentication method* for Plaintiff to access the computer as a manager and to access her paystubs as an hourly employee as a condition of her employment with White Castle." (Emphasis added.) The subsequent scans did not collect any new information from plaintiff, and she suffered no additional loss of control over her biometric information.

***10** ¶ 53 The above reading of the statute is the only one consistent with the purposes of the Act. As this court explained in *Rosenbach*, the "precise harm" the legislature was addressing was an individual's loss of the right to maintain biometric privacy. *Rosenbach*, 2019 IL 123186, ¶¶ 33-34; *McDonald*, 2022 IL 125611, ¶ 24. And in *Krishna*, 2021 IL 125978, ¶ 46, this court stated that the Act "protects a secrecy

interest," such as an individual's right to "keep his or her personal identifying information like fingerprints secret."[3] An individual loses his or her privacy in and control over biometric information upon the first scan. At this point his or her secrecy interest is lost—he or she may no longer keep his or her personally identifying information a secret from the private entity. Once that entity has the fingerprint, there is no additional loss of control, loss of privacy, or loss of secrecy from subsequent scans of the same finger. This is true whether the same finger is scanned a few times or one million times. The individual loses control over it only once. Accordingly, under *Feltmeier*, a section 15(b) claim accrues the first time a scan is taken without the required disclosures and consent. There was a single overt act from which damages flow, because the employer did not obtain anything with subsequent scans that it did not already have, and the employee did not lose control over and privacy in her biometric information with subsequent scans.

[3] The majority denies that our prior cases support White Castle's argument. The majority states that

> "*Rosenbach* does not stand for the proposition that the 'injury' for a section 15 claim is predicated on, or otherwise limited to, an initial loss of control or privacy. Instead, *Rosenbach* clearly recognizes the statutory violation itself is the 'injury' for purposes of a claim under the Act, which is entirely consistent with our decision here." *Supra* ¶ 38.

The majority assumes what it seeks to prove. The majority never explains how there is more than one loss of control or privacy with subsequent scans or how subsequent scans are a "statutory violation."

¶ 54 Thus, I agree with White Castle's argument on appeal: "Plaintiff's injury under [section] 15(b) occurred, if at all, the first time that her biometrics were collected by White Castle without her consent, not each subsequent time that her finger was rescanned." There is only *one* loss of control or privacy, and this happens when the information is first obtained. Indeed, the legislative findings in the Act confirm this. See 740 ILCS 14/5(c) (West 2018) ("[S]ocial security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, *once compromised, the individual has no recourse* ***." (Emphasis added.)). The majority tellingly never explains how there is any additional loss of control or privacy with subsequent scans that are used to compare the employee's fingerprint with the fingerprint that White Castle already possesses. The majority simply asserts that every scan is a collection and therefore a violation of the Act. *Supra* ¶ 24. And this is the key flaw in the majority's analysis: it begs —rather than answers—the most important question before the court.

¶ 55 The analysis is the same for section 15(d) claims. Under section 15(d), a private entity in possession of a person's biometric identifier or information must obtain that person's consent before it may "disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(d) (West 2018). With respect to any one party to whom the biometric information is disclosed, the person loses control of her biometric identifier or information only once. There is no further loss of control, privacy, or secrecy with subsequent provision of the identical biometric information to the same party.

¶ 56 The majority reaches the conclusion that section 15(d) includes repeated transmission to the same party (*supra* ¶ 28) only when willing to ignore (1) the plain meaning of the word "disclose" and (2) the way in which the Illinois legislature consistently uses the word "redisclose." The word "disclose" means "to make known" or "to reveal *** something that is secret or not generally known" (Webster's Third New International Dictionary 645 (1993)) or "[t]o make (something) known or public," "to reveal" (Black's Law Dictionary 583 (11th ed. 2019)); see also *Cothron v. White Castle System, Inc.*, 20 F.4th 1156, 1163 (7th Cir. 2021) (explaining that "the ordinary meaning of 'disclose' connotes a new revelation" (citing Black's Law Dictionary (11th ed. 2019))). With respect to a disclosure to any one party, this is obviously something that can happen only once. You can tell someone your middle name an unlimited number of times, but you can disclose it to them only once. Therefore, when something is "redisclosed" or "disclosed again," it must be to *a different party*. As the Seventh Circuit explained, "[r]epeated transmissions of the

same biometric identifier to the same third party are not new revelations." *Cothron*, 20 F.4th at 1163.

***11** ¶ 57 Although the majority holds that it need not determine the meaning of "redisclose" in section 15(d) (*supra* ¶ 28), the definition of "redisclose" found in the WordSense Dictionary, https://www.wordsense.eu/redisclose/ (last visited Jan. 7, 2023) [https://perma.cc/63VU-RRTK] ("[t]o disclose again; *to disclose what has been disclosed to the discloser*" (emphasis added)) is consistent with how the term is used by the Illinois legislature. See *Cothron*, 20 F.4th at 1164. As noted by the majority, the Seventh Circuit gave two examples: section 35.3(b) of the Children and Family Services Act (20 ILCS 505/35.3(b) (West 2020) ("[a] person to whom disclosure of a foster parent's name, address, or telephone number is made under this Section shall not redisclose that information except as provided in this Act or the Juvenile Court Act of 1987")) and section 5 of the Mental Health and Developmental Disabilities Confidentiality Act (740 ILCS 110/5(d) (West 2020) ("[n]o person or agency to whom any information is disclosed under this Section may redisclose such information unless the person who consented to the disclosure specifically consents to such redisclosure")). *Supra* ¶ 28 n.2; *Cothron*, 20 F.4th at 1164. In its reply brief, defendant lists several other Illinois statutes that use the term "redisclose" in the same manner.

¶ 58 Thus, if we consider the plain meaning of the word "disclose" and the manner in which the legislature consistently uses the term "redisclose," it is clear that section 15(d)'s use of the word "redisclose" does *not* mean repeated disclosures to the same party (a logical impossibility) but rather refers to downstream disclosures to third parties. In other words, if the party in possession of biometric information discloses it to a third party, consent is required before that third party rediscloses the information to anyone else. Plaintiff's only response to this argument is to claim that this interpretation renders the word "redisclose" in section 15(d) superfluous or redundant, as any disclosure to a new party would be covered by the word "disclose." But all that plaintiff can demonstrate with this argument is that the word "redisclose" is probably unnecessary in the English language (perhaps why Webster's does not define it). In the other statutes quoted above, the legislature could have used "disclose" instead of "redisclose," and the meaning of the provisions would not change. But the reality that plaintiff cannot avoid is that (1) the legislature consistently uses the term "redisclose" to mean "to disclose what has been disclosed to the discloser" and (2) a "redisclosure" to the same party is a logical impossibility.

¶ 59 The majority acknowledges that, in construing the Act as it has, the consequences may be harsh, unjust, absurd, or otherwise unwise. *Supra* ¶ 40. In doing so, the majority ignores that the construction of a statute that leads to an absurd result must be avoided. *Mulligan v. Joliet Regional Port District*, 123 Ill. 2d 303, 312-13 (1988). Instead, a court construing the language of a statute should

> " 'assume that the legislature did not intend to produce an absurd or unjust result' (*State Farm Fire & Casualty Co. v. Yapejian*, 152 Ill. 2d 533, 541 (1992)), and [should] avoid a construction leading to an absurd result, if possible (*City of East St. Louis v. Union Electric Co.*, 37 Ill. 2d 537, 542 (1967))." *Hubble v. Bi-State Development Agency of the Illinois-Missouri Metropolitan District*, 238 Ill. 2d 262, 283 (2010).

¶ 60 In considering the consequences of construing the Act one way or another and giving each word of the statute a reasonable meaning (*Haage v. Zavala*, 2021 IL 125918, ¶ 44), two significant consequences militate against the majority's construction. First, under the majority's rule, plaintiffs would be incentivized to delay bringing their claims as long as possible. If every scan is a separate, actionable violation, qualifying for an award of liquidated damages, then it is in a plaintiff's interest to delay bringing suit as long as possible to keep racking up damages. Because there is no additional loss of privacy, secrecy, or control once a private entity has obtained a person's biometric information, the plaintiff loses nothing by waiting to bring suit until as many scans as possible are accumulated. This point, all by itself, should convince the majority that its interpretation is wrong. If, indeed, a party *was* losing control over his or her biometric information with every scan, this incentive would simply not exist.

***12** ¶ 61 Next, the majority's construction of the Act could easily lead to annihilative liability for businesses. As the Seventh Circuit explained:

> "White Castle reminds us that the Act provides for statutory damages of $1,000 or $5,000 for 'each violation' of the statute. § 14/20. Because White Castle's employees scan their fingerprints frequently, perhaps even multiple times per shift, Cothron's interpretation could yield staggering damages awards in this case and others like it. If a new claim accrues with each scan, as Cothron argues, violators face potentially crippling financial liability." *Cothron*, 20 F.4th at 1165.

The majority acknowledges White Castle's estimate that, if plaintiff is successful in her claims on behalf of as many as 9500 current and former White Castle employees, damages in this action may exceed *$17 billion*. *Supra* ¶ 40. Nevertheless, the majority brushes this concern aside by stating that "policy-based concerns about potentially excessive damage awards under the Act are best addressed by the legislature." *Supra* ¶ 43.

¶ 62 However, we are not being asked to render a decision on the damages in this case or to make a policy-based decision about excessive damages. Rather, we are being asked to determine legislative intent by considering the consequences of construing the statute one way or another. Surely the potential imposition of crippling liability on businesses is a proper consequence to consider. When the plaintiff argued in the Seventh Circuit that the calculation of damages is separate from claim accrual, that court pointed out that plaintiff "does not explain how alternative theories of calculating damages might be reconciled with the text of section 20." *Cothron*, 20 F.4th at 1165. Given that plaintiff argues that every scan is a violation and the statute sets forth what an aggrieved person may recover for "every violation," it is certainly proper to consider the consequences of plaintiff's interpretation of the statute.

¶ 63 Imposing punitive, crippling liability on businesses could not have been a goal of the Act, nor did the legislature intend to impose damages wildly exceeding any remotely reasonable estimate of harm. Rather, the legislature recognizes that the use of biometrics is an emerging area whose ramifications are not completely known and that it is in the public interest to regulate the "collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5 (West 2018). Indeed, the statute's provision of liquidated damages of between $1000 and $5000 is itself evidence that the legislature did not intend to impose ruinous liability on businesses. Moreover, the majority's interpretation would lead to the absurd result that an entity that commits what most people would probably consider the worst type of violation of the Act—intentionally selling their biometric information to a third party with no knowledge of what the third party intended to do with it—would be subject to liquidated damages of $5000, while an employer with no ill intent that used that same person's fingerprint as an authentication method to allow access to his or her computer could be subject to damages hundreds or thousands of times that amount. This could not have been the legislature's intent.

***13** ¶ 64 The majority fails to set forth any similar dire consequences with White Castle's interpretation. With respect to control, the individual does not lose all control over his or her biometric data. Consent is still required before the private entity may disclose it to anyone else (*id.* § 15(d)), and that is the real concern once an individual has consented to a private entity collecting a biometric identifier or information. With respect to postcollection, White Castle correctly explains:

> "[T]he Privacy Act itself contains numerous provisions that serve its prophylactic goals even after the first collection or disclosure. Specifically, White Castle has a duty to safeguard information it has collected. 740 ILCS 14/15(a), (e). White Castle has an ongoing duty to destroy any biometric data that current employees have already scanned, once the data's purpose is fulfilled. *Id.* at 15(a). Section 15(c) prohibits the sale of biometrics, so any sale of biometrics would give rise to a new claim. *Id.* at 15(c). Section 15(d) prohibits the disclosure of biometrics to a third party without consent. *Id.* at 15(d). So disclosure of biometrics to *a new third party* would give rise to a new claim—a straightforward reading of the statute that has *always* been White Castle's position ***." (Emphases in original.)

Thus, the Act very tightly regulates what private entities may do with the biometric information they collect, and individuals maintain a measure of control over their biometric data.

¶ 65 While discussing the strengths and weaknesses of each side's argument, the Seventh Circuit suggested two potential problems with a single accrual rule. First, that court speculated that the premise that "two violations aren't worse than one" may "simply be wrong." *Cothron*, 20 F.4th at 1165. The court speculated that "[r]epeated collections or disclosures of biometric data, even if by or to the same entity, might increase the risk of misuse or mishandling of biometric data." *Id.* This assumes, however, that repeated *scans* of the same biometric identifier by the same entity are repeated "*collections*" or "*disclosures*," which is a dubious proposition. Indeed, the Seventh Circuit itself had earlier explained that a disclosure is a "new revelation" and that "[r]epeated transmissions of the same biometric identifier to the same third party are not new revelations." *Id.* at 1163. Moreover, there is no reason to believe that subsequent scans of the same biometric identifier used *for authentication purposes* against a stored copy would increase the risk of misuse or mishandling of biometric data. Second, the Seventh Circuit speculated that, under a single accrual rule, "[o]nce a private entity has violated the Act, it would have little incentive to course correct and comply if subsequent violations carry no legal consequences." *Id.* at 1165. The Act, however, provides for injunctive relief. See 740 ILCS 14/20(4) (West 2018); see also *McDonald*, 2022 IL 126511, ¶ 6 ("McDonald and the putative class sought (1) injunctive and equitable relief to protect their interests by requiring Bronzeville to comply with the Privacy Act's requirements."). Moreover, there is no reason to believe that an employer would rather be on the hook for liquidated damages to every new employee it hires rather than simply providing the notice and obtaining the consent that the Act requires. Finally, as White Castle points out:

> "Plaintiff purports to allege two violations of the Act, for up to 9,500 current and former White Castle employees. Even under a single accrual method, damages could equate to between $19 million and $95 million if Plaintiff's claims had been timely made, assuming that Plaintiff could recover separately under Section 15(b) and 15(d). Even under a 'one violation per employee' calculation of $1,000 per employee, damages could equal $9.5 million. These numbers, in and of themselves, are sufficient to incentivize [Act] compliance."

***14** The consequences of construing the statute to provide multiple accruals are severe, and neither plaintiff nor the majority has identified similar severe consequences to White Castle's interpretation.

¶ 66 In sum, the Act's legislative findings and intent show that the legislature recognized the utility of biometric technology and wanted to facilitate its safe use by private entities by regulating how it is used. See 740 ILCS 14/5(a) (West 2018) ("The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings."). The Act thus requires notice and consent before biometric information is collected or disclosed. To encourage compliance and to prevent and deter violations, the Act provides for injunctive relief and liquidated damages. I see nothing in the Act indicating that the legislature intended to impose cumbersome requirements or punitive, crippling liability on corporations for multiple authentication scans of the same biometric identifier. The legislature's intent was to ensure the safe use of biometric information, not to discourage its use altogether.

¶ 67 CHIEF JUSTICE THEIS and JUSTICE HOLDER WHITE join in this dissent.

All Citations

--- N.E.3d ----, 2023 IL 128004, 2023 WL 2052410

End of Document